WHAT IS CLAIMED IS:

1. A MAC (media access control) address-based communication restricting method comprising the steps of:

receiving packet data upon request of communication through at least one port of a plurality of ports of an Ethernet switch;

reading a MAC destination address and a MAC source address included in the received packet data;

detecting, in an address table, access vectors corresponding to the MAC destination and source addresses; and

denying access if the access vectors of the MAC destination and source addresses are not matched.

2. The method as set forth in claim 1, further comprising steps of:

configuring an anti-hacker table comprising information pertaining to a plurality of client nodes and a plurality of server nodes of a network, wherein each client node is identified by a corresponding MAC address, a corresponding host identification and a corresponding IP (Internet protocol) address, and each server node is identified by a corresponding MAC address, a corresponding host identification and a corresponding IP (Internet protocol) address;

determining whether the received MAC source address is stored in said address table;

configuring an address entry for said received MAC source address when it is determined that said MAC source address is not stored in said address table and identifying said received MAC source address as a new MAC source address;

determining whether said new MAC source address is stored in said anti-hacker table; and

storing the configured address entry for said received MAC source address in said address table when it is determined that said new MAC source address is not stored in said anti-hacker table.

3. The method as set forth in claim 2, further comprising steps of:

adding a port number, corresponding to the port through which said packet data was received, to a storage area corresponding to said new MAC source address in said anti-hacker table, when it is determined that said new MAC source address is stored in said anti-hacker table;

modifying an access vector included in said configured address entry for said new MAC source address, to set security; and

storing the configured address entry including the modified access vector for said new MAC source address in said address table.